National Infrastructure Protection Center
CyberNotes

Issue #23-99 *November 10, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 22, and November 4, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Alibaba[1]	Alibaba Web Server 2.0	Alibaba Web Server is vulnerable to path climbing, and also is vulnerable to an attack that allows the execution of arbitrary commands on the remote server. Using specially formed URL's, a malicious user can list, view, create, delete, and/or execute any file.	No workaround or patch available at time of publishing.	Alibaba Multiple CGI Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[1] SecurityFocus, October 28, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Apple[2]	MacOS 9.0	It is possible to bypass the console lock mechanism of the operating system, by using a special sequence of buttons. A malicious user can also interrupt the idle screen by using the programmer's switch; this drops you into the micro-debugger, which allows you to kill the idle screen.	No workaround or patch available at time of publishing.	Console Lock and Programmer's Window Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Avirt [3]	AVirt Gateway Suite 3.3a, 3.5	Remotely exploitable buffer overflow vulnerability exists in the Avirt Mail Server 3.3a and a denial-of-service vulnerability exists in version 3.5, (long USER / PASS:) that may allow an attacker to execute arbitrary code on the target server. Also it contains a weakness in the code that handles the RCPT TO command that could cause the mail server to create a directory in the server's local filesystem.	No workaround or patch available at time of publishing.	AVirt Mail Server Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Axent[4]	Raptor 6.0 Firewall	It is possible to remotely lock Axent Raptor firewalls by sending packets with malformed IP options fields. A consequence of this is a remote denial of service. **Each site should determine whether systems protected by Raptor Firewall are mission critical.**	Axent has released a hot fix: ftp://ftp.raptor.com/patches/V6.0/6.02Patch/	Denial of Service Vulnerability	**High (Due to the potential systems affected)**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[2] SecurityFocus, October 26, 1999.
[3] SecurityFocus, October 31, 1999.
[4] Securityportal, October 21, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BlueFace[5]	BlueFace Falcon Web Server 1.0	Falcon Web Servers suffer from a path parsing problem, which allows a remote user to escape out of the webroot directory. Remote users have the ability to view directory paths, download files (depending on permissions), and may use this to compromise the web server.	FWS version 1.0.0.1008 fixes the vulnerabilities and is available at: http://www.blueface.com/products.html#fws	Falcon Web Server Directory Traversal Vulnerability	Medium	Bug discussed in newsgroups and websites.
BTD Studio[6]	Zom-Mail 1.0.9	Certain versions of the BTD Zom-Mail server contain a buffer overflow, which may be remotely exploitable by malicious users.	No workaround or patch available at time of publishing.	Xom-Mail Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
ByteFusion[7]	ByteFusion's BFTelnet Server 1.1	A buffer overflow vulnerability exists that can easily lead to a Denial-of-Service attack.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press.
Caltech Software[8]	Caltech Software ExpressFS 2.6	A buffer overflow vulnerability exists that allows a Denial-of-Service attack, and possibly execution of arbitrary code.	No workaround or patch available at time of publishing.	ExpressFS USER Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
CISCO[9]	CISCO NAT	It is possible to cause a connection to the router to be dropped by sending a manual PORT command. This will cause the router to reroute the connection and thus drop it.	No workaround or patch available at time of publishing.	CISCO NAT Denial-of-Service	Low	Bug discussed in newsgroups and websites.
ETYPE[10]	Eserv 2.50	An unauthorized user can gain read access to any file on the system, including account files, by entering a specific string in a URL.	No workaround or patch available at time of publishing.	Eserv 2.5 Directory Traversal Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published. **Trojan Horse program exist that looks for the specific port.**

[5] BindView Security Advisory, October 24, 1999.
[6] SecurityFocus, November 3, 1999.
[7] NT Security, November 4, 1999.
[8] SecurityFocus, October 29, 1999.
[9] SecurityFocus, November 5, 1999.
[10] NTBUGTRAQ, November 4, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Floosietek[11]	FTGate 2.1	An unauthorized user can gain read access to any file on the system, including account files, by entering a specific string in a URL.	No workaround or patch available at time of publishing.	FTGate 2.1 Directory Traversal Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published. **Trojan Horse program exist that looks for the specific port.**
FreeBSD 3.0, 3.1, 3.2, 3.3[12]	Hylafax 4.0.2	Vulnerability exists in 'faxalter' that allows any user to gain uucp and possibly root privileges by overflowing the buffer.	No workaround or patch available at time of publishing.	'Faxalter" Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett-Packard[13]	HP-9000 Series 700/800, HP-UX releases 10.X and 11.00	Vulnerability exists in automountd, which can run user programs as root. Originally released in June this root compromise vulnerability has been re-released because of the large number of systems still affected and the addition of vendor information from HP. HP has released an advisory indicating automountd, which was previously thought to immune from the recent automountd bugs affecting other platforms, is also vulnerable.	At this time there are no patches available for any releases. As a work around, setting AutoFS = 0 in the file /etc/rc.config.d/nfsconf, will disallow most exploitations.	Automountd Root Compromise Vulnerability	**High**	Bug discussed in newsgroups and websites.
IBM[14]	AIX 4.3.2	Due to the way AIX filtering services work, a remote user can access services which listen on non-privileged ports higher than 32767.	No workaround or patch available at time of publishing.	AIX Filtering Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[15]	HomePage Print 1.07	If a page containing a specially constructed IMG SRC tag is previewed or printed using the IBM HomePagePrint software, arbitrary code can be run on the client.	Patch is available at: http://www.ibm.co.jp/software/internet/hpgprt/down2.html	HomePage Print Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts has been published.

[11] Ussr Labs, November 5, 1999.
[12] Securiteam, November 5, 1999.
[13] Hewlett-Packard Company Security Advisory: #00104, October 21, 1999.
[14] Bugtraq, October 25, 1999.
[15] SecurityFocus, November 3, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
IBM[16]	WebSphere HTTP Server	IBM's HTTP Server stores the password to your private SSL key in a "stash" file, which can be retrieved and cracked. The password can then be used to gain access to the private SSL certificates.	No workaround or patch available at time of publishing.	SSL Key Password Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Linux[17]	Linux 2.2.13	Linux systems can sent forged packets even when protected from the outside interfaces by firewalling rules. Most of the time, these packets bypass existing firewalling rules. This attack requires only a shell account on the system.	No workaround or patch available at time of publishing.	IP Spoofing Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Linux[18]	RedHat Linux 6.1	The version of screen that ships with Redhat Linux 6.1 incorrectly sets permissions on the pty (pseudo-terminal driver). As a result of these permission settings, pty's are world writable, which can result in root privileges if 'root' is running the vulnerable version of screen.	Patch can be found at: ftp://ftp.redhat.com/pub/redhat/updates/6.1/i386/screen-3.9.4-3.i386.rpm Please replace i386 with the appropriate architecture for your system.	Insecure PTY Permissions Vulnerability	**High**	Bug discussed in newsgroups and websites.
Linux[19]	RedHat, Debian, and SuSE releases	Ypserv releases previous to 1.3.9 contain two different vulnerabilities: Any NIS domain administrator can inject password tables, and users can modify the GECOS field and login shell values for other users. Also, rpc.yppasswd prior 1.3.6.92 has a standard buffer overflow problem in the md5 hash generation code.	Please contact your vendor for the current patch.	Multiple Vendor Linux NIS Vulnerabilities	Medium/ Low	Bug discussed in newsgroups and websites. Exploit has been published.

[16] Securiteam, October 26, 1999.
[17] SecurityFocus, October 27, 1999.
[18] RedHat Security Advisory, RHSA-1999:042-01, October 20, 1999.
[19] SecurityFocus, November 1, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[20]	Hotmail	Vulnerability in Microsoft's Passport service opens a security hole that exposes Netscape 4.0 and higher (and possibly Internet Explorer) users using the Hotmail mail service. By making a settings change in Netscape, the next user that tries to logon to Hotmail (on that same machine) has complete access to the previous user's mailbox.	No workaround or patch available at time of publishing.	Passport Sign-Out Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft Windows[21] ***Patch has been released.[22]***	**Internet Explorer; Outlook E-mail**	**Vulnerability exists in Java Virtual Machine, which could enable a malicious programmer to take control of the victim's computer. A malicious applet could also be embedded in an e-mail message.**	**No workaround or patch available at time of publishing.** ***Patches that eliminate this vulnerability can be downloaded at:*** http://windowsupdate.microsoft.com	**Java Virtual Machine Vulnerability**	**High**	**Bug discussed in newsgroups and websites.**
Microsoft Windows 95, 98, NT 4.0[23]	Internet Explorer 4.0, 5.0; Outlook 98.0	IE 4.0 and 5.0 allows reading local text and HTML files, and files from any domain. Window spoofing is possible and in some cases, it is also possible to read files behind a firewall.	No workaround or patch available at time of publishing. Temporary workaround: Disable active scripting.	IE Window.open Redirect Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[20] Bugtraq, October 21, 1999.
[21] Bugtraq, October 14, 1999.
[22] Microsoft Security Bulletin (MS99-045), October 21, 1999.
[23] Securiteam, November 4, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 95, 98, NT 4.0 NT 2000[24] ***Regression error in IE hotfixes..***[25]	**Internet Explorer 4.0.1, 5.0** ***Internet Explorer 5.0***	**Internet Explorer (IE) 5 will allow a malicious web page to read the contents of local files through a weakness in the IE5 security model. Normally the document.execCommand method is restricted from reading and returning data on the local machine, however if the method is called from within an IFRAME this restriction can be circumvented.** ***There is a regression error in hotfixes for Internet Explorer 5.0. Applying the 'IFRAME ExecCommand' fix (MS99-042) will undo the 'MSHTML Update' (MS99-012). Bulletin MS99-042 has been re-released to provide a corrected version of the patch***	**Microsoft has released patches for IE 4.0.1 and IE 5. The IE 4.0.1 patch is included as part of the IE 4.0.1 Service Pack 2 available at:** **http://www.microsoft.com/windows/ie/download/windows.htm** **The IT5 patch is available as an individual fix from:** **Intel:** **ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/IE50/MSHTML-fix/x86/q243638.exe** **Alpha:** **ftp://ftp.microsoft.com/peropsys/IE/IE-Public/Fixes/usa/IE50/MSHTML-fix/Alpha/q243638.exe** ***More information and the patch can be found at:*** http://www.microsoft.com/security/bulletins/ms99-042.asp	**IE5 IFRAME Vulnerability**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Microsoft Windows NT 4.0[26] ***Microsoft issues a fix.***[27]	**Microsoft TCP/IP Stack for NT 4.0 up to and including SP3**	**Windows NT 4 uses predictable TCP sequence number generating algorithms that could allow an attacker to set up connections to other machines with a spoofed source address of the NT host.**	**No workaround or patch available at time of publishing.** ***Patch available at:*** **http://www.microsoft.com/security/bulletins/ms99-046.asp**	**TCP/IP Sequence Numbering Vulnerability**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[24] Microsoft Security Bulletin, MS99-042, October 11, 1999.
[25] Microsoft Security Bulletin, MS99-042, re-released November 4, 1999.
[26] Securiteam, August 28, 1999.
[27] Microsoft Security Bulletin, MS99-046, October 22, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows NT 4.0[28]	Windows NT 4.0 Workstation, Server, Server, Enterprise Edition, Server Terminal Edition	A security vulnerability exists that could allow a user to cause the print spooler server to crash, or to run arbitrary code on Windows NT machines.	Microsoft has released patched for NT 4.0 Server and Workstation machines are at SP5 or SP6. Other SP levels will be supported at a later date. The patches are available for download at: X86: http://download.microsoft.com/download/winntsrv40/Patch/Spooler-fix/NT4/EN-US/Q243649.exe Alpha: http://download.microsoft.com/download/winntsrv40/Patch/Spooler-fix/ALPHA/EN-US/Q243649.exe	Malformed Spooler Request Vulnerability	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft Windows NT 4.0[29]	Windows NT 4.0, SP1, SP3, SP5, SP6	Services.exe can be made to crash, which impairs most functions of the box, including logon, logoff, file-sharing, user authentication, etc. IIS servers still respond to requests, but give out 'Not Authenticated' errors. If this Denial of Service is combined with a number of other exploits, it may be possible to have this attack spawn a Debugger call on the host, which, if trojaned, may execute malicious code on the target host.	No workaround or patch available at time of publishing. Unofficial workaround is to block port 139. This will disable outside attacks but will still leave the system vulnerable to insiders.	Services.exe Denial of Service Vulnerability	High	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Netscape[30]	Netscape 4.5 & above	A Denial-of-Service vulnerability exists in the Dynamic Font support in Netscape.	Unofficial workaround until a new version of the browser is released: Disable Dynamic Font support. That option is in Edit, Preferences, Appearance, Fonts. Make sure "Use document-specified fonts, including Dynamic Fonts" is unchecked.	Dynamic Font Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published. Exploit has appeared in the Press
Netscape[31]	Netscape Messaging Server 3.54, 3.55, 3.6	A remote attacker can cause the Netscape Messaging Server to consume 100% of the computer's memory, bringing the server to Its knees.	Netscape has stated a release date of December 1999 for Messaging Server 4.15, which will not include this vulnerability.	Messaging Server RCPT TO Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[28] Microsoft Security Bulletin, MS99-047, November 4, 1999.
[29] SecurityFocus, October 31, 1999.
[30] Whitehats, October 24, 1999.
[31] SecurityFocus, October 29, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Omnicron[32]	OmniHTTPD 1.1, 2.4Pro	There is a remotely exploitable buffer overflow vulnerability in the CGI program "imagemap", which can allow for arbitrary code to be executed on the machine running the server.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Pacific Software[33]	Pacific Software URL Live! 1.0	The URL Live! Free webserver software is susceptible to the "../" directory traversal vulnerability which allows a malicious user to gain read access to files outside the intended web file structure.	No workaround or patch available at time of publishing.	URL Live! Directory Transversal Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Real Networks[34]	Real Networks Real Server G2 1.0	There is a buffer overflow vulnerability in the web authentication on the RealServer administrator port. By sending a long user/password pair a malicious user can overflow the buffer and execute arbitrary code.	No workaround or patch available at time of publishing. Temporary workaround: Disable web administration.	Real Server Administrator Port Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published. Vulnerability has appeared in the Press.
RedHat[35] ***RedHat issues new packages.[36]***	**Red Hat Linux 4.x, all architectures Red Hat Linux 5.x, all architectures Red Hat Linux 6.x, all architectures**	**Lpr packages contain several vulnerabilities, which may allow printing of files for which read access is not allowed. The first of the two problems is a race condition that can be exploited between the access checking and the opening of the file. The second is a symlink attack that could also be used to print files that normally cannot be read by a regular user.** ***The original security patch broke some aspects of printing. New errata RPMs are available which should fix the problem.***	**Patches available at: ftp://ftp.redhat.com/pub/redhat/updates/ Select the appropriate version of Linux and the architecture for your system.** ***New patches available at:*** ftp://updates.redhat.com/ ***Please select the appropriate version of Linux and the architecture for your system.***	**Lpr/Lpd File Access Vulnerabil-ities**	**Medium /Low**	**Bug discussed in newsgroups and websites.**

[32] SecurityFocus, October 22, 1999.
[33] SecurityFocus, October 28, 1999.
[34] NT Security, November 4, 1999.
[35] RedHat Security Advisory, RHSA-1999:041-01, October 17, 1999.
[36] RedHat Security Advisory, RHSA-1999-041-03, October 25, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
SCO Unix[37]	SCO OpenServer 5.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5	Multiple vulnerabilities	Patches have been issued for multiple vulnerabilities. Cover letters explaining what the patches do are available at ftp://ftp.sco.com/SSE/sse037.ltr	UserOsa Symlink Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
SkyCommun-ications[38]	SkyCommun-ications Skyfull 1.1.4	An unchecked buffer vulnerability exists in which the argument from the MAIL FROM command is placed. This buffer can be overwritten and arbitrary code can be executed.	No workaround or patch available at time of publishing.	Mail Server MAIL FROM Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Texas Imperial Software[39]	Texas Imperial Software WFTPD 2.34, 2.40	A buffer overflow has been found in WFTPD versions 2.34 and 2.40 that may lead to a Denial of Service or even execution of arbitrary code.	No workaround or patch available at time of publishing.	WFTPD Remote Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Unix[40]	FreeBSD 3.3	The Amanda backup package has a several vulnerabilities which will allow any user to gain root privileges.	No workaround or patch available at time of publishing.	Amanda Security Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix[41]	HP-UX 10.20, 11.0; IBM AIX 4.1, 4.2, 4.3; SCO Unixware 7.0; Sun Solaris 2.5, 2.5_x86, 2.5.1, 2.5.1_x86, 2.6, 2.6_x86	Due to improper checking of ownership, the dtappgather utility shipped with the Common Desktop Environment (CDE) allows arbitrary users to overwrite any file present on the filesystem, regardless of the owner of the file. An additional vulnerability exists whereby dtappgather blindly uses the contents of the DTUSERSESSION environment variable.	A temporary measure is to remove the setuid bit from the dtappgather application. The affected vendors each issued patches, which were documented in CERT advisory CA-98.02.	Multiple Vendor CDE Dtappgather Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Unix[42]	National Foundation Squid Web Proxy 1.0, 1.1, 2.1, 2.1	Vulnerability in Squid allows users to gain access to the web proxy using a "username/password" shifting technique.	Patch can be found at: http://squid.nlanr.net/Versions/v2/2.2/bugs/squid-2.2.stable5-newlines_in_auth.patch	Squid Web Proxy Authentication Failure Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[37] SCO Security Bulletin, 99.17, November 5, 1999.
[38] SecurityFocus, November 2, 1999.
[39] SecurityFocus, October 28, 1999.
[40] Bugtraq, October 30, 1999.
[41] Bugtraq, November 3, 1999.
[42] Securiteam, October 28, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix[43]	TurboLinux 3.5b2; SGI Irix 5.3, 6.2, 6.3, 6.4, 6.5; Sun Solaris 2.6, 2.6_x86, 7.0, 7.0_x86	Canna is a Japanese input system available as free software, which provides a unified user interface for inputting Japanese. The Canna subsystem on certain Unix versions contains a buffer overflow in the 'canuum' and 'uum' programs, which will result in a root level compromise.	No workaround or patch available at time of publishing.	Canna Subsystem Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Unix[44]	Zeus Web Server 3.3.x	Several vulnerabilities exist in the Zeus Web server. Zeus' included search engine lets a remote attacker read any file on the system (restricted by permissions of the Web server). It is possible to read the Zeus configuration file and obtain the password for the administration Web server (on Port 9090), which typically runs under root context. There a malicious user can run upload scripts and binaries as root.	Zeus Technology has released new binaries for their webserver which are not vulnerable to this problem. They are available at the location below: http://support.zeus.co.uk/news/exploit.html Users who are upgrading from version 3.1.9 or earlier should follow the upgrade steps at the following URL: http://support.zeus.co.uk/faq/entries/z33migrate.html	Zeus Web Server Remote Root Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Windows[45]	AN AN-HTTPd 1.2b	Certain versions of the AN-HTTPd server contain default CGI scripts that allow code to be executed remotely. This is due to poor sanity checking on user-supplied data.	No workaround or patch available at time of publishing.	AN-HTTPd CGI Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Yamaha[46]	Yamaha MidiPlug 1.1b-j for Internet Explorer 4.0, 5.0	MidiPlug contains a buffer overflow vulnerability, which may allow arbitrary code to be executed on the local host.	No workaround or patch available at time of publishing. Temporary workaround: Disable "Run Active X controls and plugins."	Yamaha MidiPlug Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

[43] SecurityFocus, November 2, 1999.
[44] SecurityFocus, October 25, 1999.
[45] SecurityFocus, November 3, 1999.
[46] SecurityFocus, November 3, 1999.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between October 21, and November 4, 1999, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 66 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
November 5, 1999	**Eserv.txt**	**Explanation and sample URL query that exploits the Traversal Vulnerability in Eserv 2.50.**	
November 5, 1999	**FTGate.web.txt**	**Explanation and sample URL query that exploits the Traversal Vulnerability in FTGate 2.1.**	
November 5, 1999	**Falcon-ssh-diffs.tar.gz**	**Program containing two Rootkits for ssh-1.2.27. These programs disable all logging and have a magic log-in for all accounts.**	
November 4, 1999	**Alibaba.pl**	**Exploit script that will provide a directory listing of the CGI directory for Alibaba.**	
November 4 , 1999	**Hyla.c**	**Exploit script for the 'faxalter' buffer overflow vulnerability.**	
November 4, 1999	**Rau.c**	**Unix exploit script that will open a command prompt on port 6968 and exploits the Real Server buffer overflow vulnerability.**	
November 4, 1999	**Spoolsploit.zip**	**Exploit script for the Windows NT spooler vulnerability.**	
November 4, 1999	**Spoolss.c**	**Exploit script for the Windows NT Spooler vulnerability.**	
November 4 1999	**Wftp.dexp.tgz**	**A WFTPD 2.34 exploit script for WIN NT 4.0 [SP3-4], Windows 95, and Windows 98.**	
November 3, 1999	**Cgi-check99.3.r**	**Checks for 97 remote CGI vulnerabilities.**	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
November 3, 1999	Dethor.zip	Remotely crashes the Deep Throat Trojan client.	
November 3, 1999	**Ex_homepageprint.c**	**This exploit will generate an HTML document that contains an IMG SRC tag that will overflow the buffer. It works on Windows 98 clients.**	
November 3, 1999	**Ex_midiplug.c**	**Exploit script for the buffer overflow vulnerability in MidiPlug.**	
November 3, 1999	Icq.txt	ICQ Security Tutorial version 1.3. Learn how to spoof messages, get passwords to accounts; access people's file system, etc. all through ICQ.	
November 3, 1999	Icqtrp01.zip	Patched version of ICG Trojan for Windows platforms. Remote control that AVP 3.0 will not detect.	
November 3, 1999	NSS_23.tar.gz	Narrow Security Scanner is a perl script, which checks for 168 remote vulnerabilities.	
November 3, 1999	**Realown.asm**	**Asm source code for the Windows NT RealServer buffer overflow vulnerability.**	
November 3, 1999	**Realown.exe**	**Buffer overflow exploit for the RealServer administrator port vulnerability.**	
November 3, 1999	Squid.exploit.txt	Remote exploit for squid-2.2-STABLE5 or below.	
November 3, 1999	Unlgj_nn45bug_css2.zip	Bug in Netscape Communicator 4.5.	
November 3, 1999	**Zome.c**	**Remote buffer overflow exploit script for BTD Zom-Mail.**	
November 2, 1999	9910-exploits.tgz	New exploits for October 1999.	
November 2, 1999	**Ex_canuum.c**	**'canuum' buffer overflow exploit script for the Canna subsystem root compromise vulnerability.**	
November 2, 1999	**Ex_ssmail.c**	**Windows 98 exploit code that executes any command on the host, which is running the Skyfull Mail Server 1.1.4.**	
November 2, 1999	**Ex_uumc.**	**'uum' buffer overflow exploit script for the Canna subsystem root compromise vulnerability.**	
November 2, 1999	**Msadc2.pl**	**MSADC/RDS exploit script version 2.**	
November 2, 1999	Nessux-0.98.4.tar.gz	Security scanner is a free, open-sourced and easy-to-use auditing tool for Linux, BSD and some other systems. Performs over 250 remote security checks.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
November 2, 1999	Nsat-1.09.tgz	A bulk security scanner designed for recoverable long-time scans, optimized for speed and stability that scans and audits about 60 different services and 170 CGIs.	
November 2, 1999	Nss.tar.gz	Security scanner checks for 153 remote vulnerabilities.	
November 2, 1999	**Skyfull.c**	**Buffer overflow exploit script for the Skyfull mail server version 1.1.4 vulnerability.**	
November 1, 1999	**Amanda.backup.txt**	**Amanda exploit for FreeBSD backup package vulnerabilities.**	
November 1, 1999	**Amandax.c**	**Amanda runtar exploit yields uid=0(root) * Actually overflows tar 1.11.2 (included in FreeBSD 3.3)**	
November 1, 1999	**Avert.mailserver.remote.txt**	**Remote exploit buffer overflow script for Windows 98 and a 3.5 DoS.**	
November 1, 1999	**Avirtexp.exe and avirtsc.zip**	**Remote buffer overflow exploits for the Avirt Mail Server 3.3a and 3.5 packages.**	
November 1, 1999	B00ger-tpc.tar.gz	Remove RPC vulnerability scanner, which scans for rstatd, nfsd, ypserv, mountd, rexd, ypudated, cmsd, ttdbserver, autofsd, pcnfsd and amd vulnerabilities.	
November 1, 1999	**Expressfs.ftpserver.txt**	**Script that exploits the ExpressFS remotely exploitable buffer overflow vulnerability.**	
November 1, 1999	Pringles.c	Send spoofed ICMP packets containing user specified scripts exploit, which can be against some modems.	
November 1, 1999	**RFP9906.txt**	**Windows NT remote denial of service and compromise (RFPoison) exploit script.**	
November 1, 1999	**RFPoison.zip**	**Script that exploits NT 4.0 hosts by sending a specially crafted packet, which causes a Denial of Service, rendering local administration and network communication next to, useless.**	
October 29, 1999	Cr0n.c	CGI vulnerability scanner which checks for 97 vulnerabilities.	
October 29, 1999	**Httpd.c**	**Remote buffer overflow exploit script against the vulnerability in the CGI program "imagemap", which is distributed with Omnicron's OmniHTTPD.**	
October 29, 1999	**Rcpt2.c**	**A Denial of Service exploit script for Netscape Messaging server.**	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
October 28, 1999	Axent.dos.c	Denial of Service exploit script against Axent Raptor 6.0 IP Options. Tested on Intel/*BSD systems.	
October 28, 1999	Ethereal-0.7.7.tar.gz	GTK=-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.	
October 28, 1999	**Url.live-1.0.txt**	**Script that exploits theURL Live! 1.0 WebServer vulnerability, which allows any user to download any file on the victim, host.**	
October 28, 1999	**Wftpd.txt**	**Exploit script for the WFTPD v2.34,v2.40 Server vulnerability to remotely exploitable buffer overflow.**	
October 27, 1999	Cracking2.txt.	Cracking tutorial, which will guide you through the cracking process of a small program and help, you understand all the steps involved in cracking.	
October 27, 1999	**Floorboard.c**	**Exploit script for Linux 2.2.13 that can be used against the IP vulnerability.**	
October 27, 1999	Ftpcheck.pl	Ftpcheck version 0.32 scans hosts and networks for FTP and anonymous FTP archives.	
October 27, 1999	Raptor.c	Denial of Service exploit script that remotely locks Axent Raptor firewalls By sending them packets with malformed IP options fields.	
October 27, 1999	RFP9905.zeus_root.txt	Remote root compromise via Zeus webserver.	
October 26, 1999	LOGINW32.zip	A simple GUI Trojan that when added to the autostart “see regedit” registry will log the passwords of the Novell NetWare School Vista user to c:\windows\samples.txt.	
October 26, 1999	Nsat-1.08.tgz	A bulk security scanner designed for recoverable long-time scans, optimized for speed and stability that scans and audits about 60 different services and 170 CGIs.	
October 26, 1999	Pr0tscan-release-1.tar.gz	Based on Vetescan, but has more vulnerabilities and runs smoother.	
October 26, 1999	Spike.sh5.zip	32 Denial of Service attacks at once.	
October 26, 1999	Suidshow.c	A Linux lkm that will log any non-root user doing a setuid() or a setreuid(0.0) system call.	
October 26, 1999	Vetscan10-26-1999.tar.gz	Unix/Windows remote vulnerability exploit scanner with fixes for vulnerabilities.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
October 26, 1999	Walker.c	Compuserve 3.0 password decryptor who decrypts 3.0 ini files that stores account passwords.	
October 25, 1999	Dopewarez.c	Remote exploit for dopewars-1.4.4. Exploit works for servers as well as clients.	
October 22, 1999	Ethereal-0.7.6-tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.	
October 22, 1999	**Imagemap.cgi.txt**	**Exploit script against the CGI vulnerability in OmniHTTPd 1.01 and Pro2.04, which can execute any command on the victim host.**	
October 22, 1999	Omega.txt	Tutorial on a new way of exploiting buffer overflows.	
October 22, 1999	**OmniHTTPd.c**	**Remote buffer overflow exploit script against the vulnerability in the CGI program "imagemap", which is distributed with Omnicron's OmniHTTPD.**	
October 21, 1999	Adv.overflow.paper.txt	Paper on writing advanced buffer overflow exploits.	
October 21, 1999	Exp.dat	New updated version of database exp.dat for CGI scanner.	
October 21, 1999	Versioner-03.cpp	Versioner0.3 source code. Versioner is a command line tool that traverses directories gathering the file properties which outputs its information in a human readable text format as well as a comma separated version that can be imported directly into MS-Excel or MS-Access.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two week period:

- **Government and military sites are being compromised via vulnerabilities in IIS web servers and MS Data Access Components (MDAC) vulnerabilities. (CyberNotes 99-22)**
- The e-mail Trojan called VBS.Freelink continues to spread across the Internet.
- Two vulnerabilities are being used together to gain access to vulnerable systems. The first is rpc.statd, a program used to communicate state changes among NFS clients and servers. The second is in automountd, a program used to automatically mount certain types of file systems.
- An increased number of reports about intruders compromising machines in order to install distributed systems used for launching packet-flooding Denial of Service attacks.
- Intrusion detection systems ranging from home computers with cable modems to high-end government facilities have been reporting a large number of probes to TCP ports 80, 8080 and 3128.
- Variations of the Melissa virus continue to appear.
- Intruders are using distributed network sniffers to capture usernames and passwords. UDP packets containing username and password information may be sent to one or more remote sniffer servers using source port 21845/udp.
- Increased intruder activity has been noticed involving the am-utils package.
- An increase in widespread probes to port 21/tcp has been seen.
- Web hacks using ColdFusion vulnerabilities continue.

Viruses

P98M/Corner: A new, fairly benign virus is being described as a "proof of concept" virus by security vendors, as it is the first to infect Microsoft Project applications. It is the first macro virus to infect both Project and Word documents, and can travel between them.

The Corner virus spreads from user to user in infected Word .doc and Project .mpp files, but does not replicate itself or appear to contain a hazardous payload.

Although the virus is not dangerous, and was predicted by anti-virus vendors, companies are still keeping a close eye out for Corner because of its ability to cross-infect Project files and Word files which can be sent to other users. Microsoft Project is project management software that Microsoft claims is used by 2 million users.

When a user receives the Corner virus macro and opens it in Microsoft Word 97 or Word 2000, Corner checks if Microsoft Project is running and infects it. The Word part of the virus spreads when an infected document is closed as it then sets the Office 2000 security settings to low, disables the "Tools/Macros" menu and turns off the macro virus protection within Microsoft Office. After that the virus replicates to all opened documents. It will turn off the security checking for macros, either by modifying the registry or by disabling the virus protection within Microsoft Office. It tries to infect the global template of Microsoft Word, or Microsoft Project. The virus infects a Word application by opening it and inserting the virus code in the global template's class module "ThisDocument". This process is hidden from the user, and the user can not see the infection of Word. To infect Project, the virus adds a new blank project and inserts the virus code into the "ThisProject" class module. The virus also includes the statement:

> "I never realized the lengths I'd have to go / I'll the darkest corners of a sense / I didn't know / Just for one moment / hearing someone call / Looked beyond the day in hand / There's nothing there at all / Project98/Word97-2k Closer"

I-Worm.Badass: A new version of VBS/Monopoly.B and Trojan.Wincom has been spreading across the Internet. Requiring Outlook and libraries, version 6.0 or later, this virus is not malicious but could cause servicing or networking errors because of it's spam-like replication methodology.

W97M.BMH: The latest macro virus to strike is a Microsoft Word 97 Macro virus, which infects the global template or normal.dot of Word 97 and will infect every document opened or created on the infected system. This new virus is unique in that it not only infects the normal template but it creates a special file called SNrml.dot in the \Office\STARTUP directory.

Most macro viruses tend to infect the normal.doc template only, but the BMH virus is unique in that it creates another .dot template and it saves it in the office start up directory. As a result of that, even if you remove the virus from the normal.dot, it will come back. Every file that it's in the Office start up directory will be executed when Word starts up. It will start up and reinfect the system once again.

Once the virus infects a system it will also set the macro virus warning system within Office to the lowest setting, enabling future virus infections. It will also alter the Word application so that when users try to activate features, a picture will be shown instead. It prevents you from performing certain actions in Word. It will modify the word configuration files, so that certain menu options inside word are unavailable. It will instead of activating that option, it will display a picture instead.

W97M_Chantal.A: On any day of year 2000, this virus is capable of deleting all files in the C drive, followed by a message box displaying

"Chantal B. 4ever! Mark says…"

Whereas on the 31st day of the month, the Office Assistant conversation balloon appears with

"Mark says …" as the header and "Chantal B. 4ever!" as the test.

This virus will set the security settings of word 2000 to low level and disable macro and security controls. It will also modify entries in the registry, to change the registered owner of windows to "Chantal 4ever!" and the windows current version to "CB1999" (so that the system runs CB1999.vbs everytime it starts).

Trojans

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #99-20 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
Backdoor	0.1	CyberNotes 99-21
Bla	1.0-2.0	CyberNotes 99-22
BladeRunner		CyberNotes 99-22
Bobo		CyberNotes 99-20
BrainSpy	Beta	CyberNotes 99-21
Deepthroat	3.1	CyberNotes 99-20
Doly	1.1-1.6	CyberNotes 99-20
Donald Dick	1.53	CyberNotes 99-22
Donald Dick	1.52	CyberNotes 99-20
Eclipse 2000		CyberNotes 99-20
InCommand	1.0	CyberNotes 99-20
Ini Killer	2.0-3.0	CyberNotes 99-21
Irc3		CyberNotes 99-21
Logger		CyberNotes 99-21
Matrix	1.4-1.5	CyberNotes 99-20
Millennium	1.0-2.0	CyberNotes 99-21
Naebi	2.12-2.34	CyberNotes 99-22
NetSphere	1.0-1.31337	CyberNotes 99-20
NetSpy	1.0-2.0	CyberNotes 99-22
Phaze Zero	**1.0b - 1.1**	**Current Issue**
Revenger	**1.0**	**Current Issue**
RingZero		CyberNotes 99-22
Ripper		CyberNotes 99-22
SpiritBeta	1.2f	CyberNotes 99-22
SubSeven	1.0-2.0	CyberNotes 99-21
Thing	**1.00 - 1.60**	**Current Issue**
Transmission Scout	**1.1 - 1.2**	**Current Issue**
Vampire	**1.0 - 1.2**	**Current Issue**
WarTrojan	1.0-2.0	CyberNotes 99-21
Xplorer	1.20	CyberNotes 99-21
Y2K Countdown (Polyglot)		CyberNotes 99-20

PhazeZero (October 23, 1999): This Trojan has basic Netbus like features. It listens on TCP port 555, and like Netbus is easily removed.

Revenger (October 23, 1999): This Trojan boasts many commands, mostly Netbus like, however, can edit the registry and has a lot of commands strictly for interacting with the real user. The installation of this Trojan isn't very stealthy and it is easily removed.

Transmission Scout (October 27, 1999): This is an 'all in one' Trojan, with most all of Netbus's features, as well as additions such as a registry editor, key logger, password grabber, e-mail/ICG notify, and more.

Thing (October 20, 1999): This Trojan only has two functions. Transfer files and run programs. This Trojan is also extremely small and is usually attached to another programs installer, and used to install a more powerful Trojan on your system at a later date.

Vampire (October 19, 1999): This is a basic Trojan with many standard features, however does have some destructive features such as 'Format HD'. Its also made to run on both Windows 95/98 AND Windows NT.